كلية الحوسبة والمعلوماتية |
College of Computing and Informatics

الجامعة السعودية الإلكترونية
SAUDI ELECTRONIC UNIVERSITY
2011-1432

Semester 1 – 2021/2022

Course Code	CYS613
Course Name	Advanced Principals of Cyber Security
Assignment type	SeedLab
Module	07

Student ID	
Student Name	
CRN	15320

Solution:

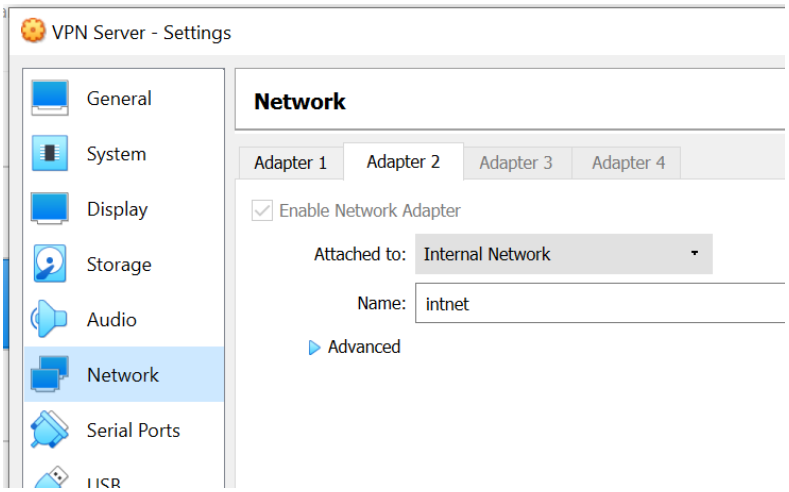
Virtual Private Network (VPN) Lab

Lab Setup

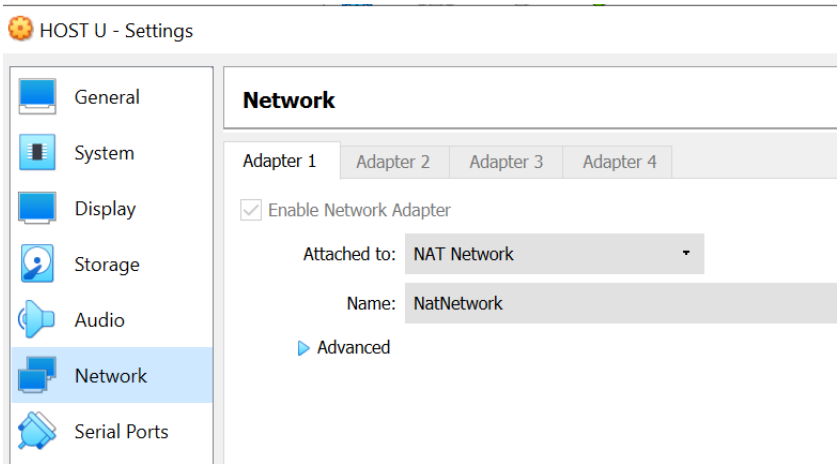
We have three machines in this lab, the VPN server, host U and host V. Hoste V will be the isolated machine, and we will try to make hos U communicate with the isolated machine host V.

First, we will make the environment ready by having three machines and setup the network cards for each machine as follow:

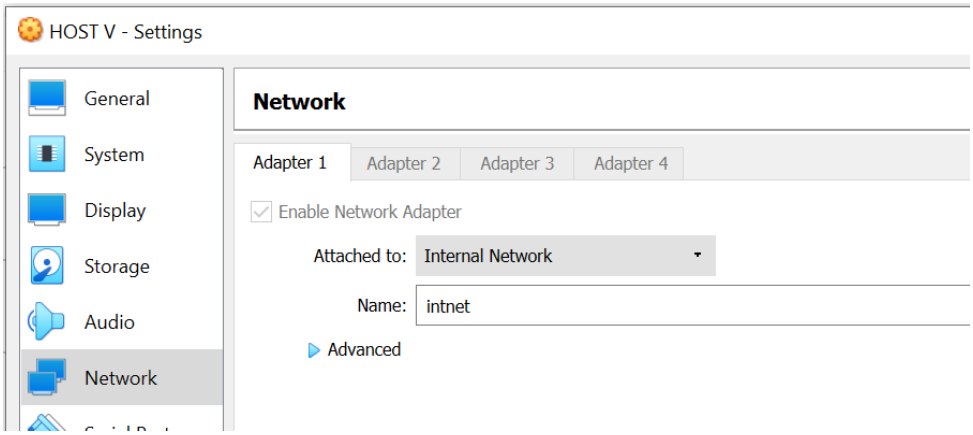
The VPN server will have two Network adapters:

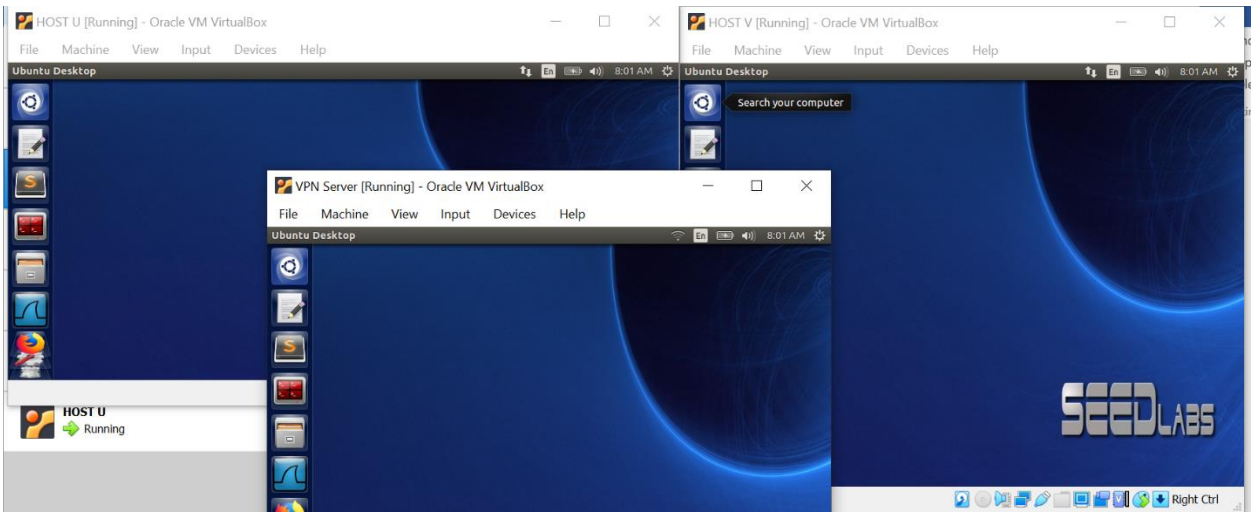


Hots U

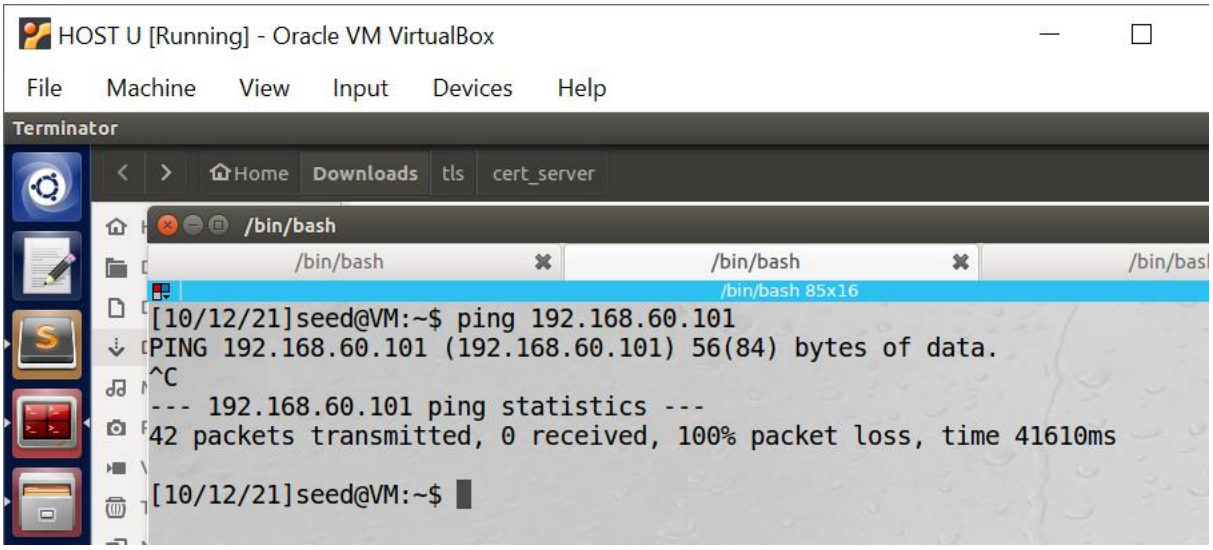

HOST U - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
NAT Network
Name:
NatNetwork
Advanced

Host V

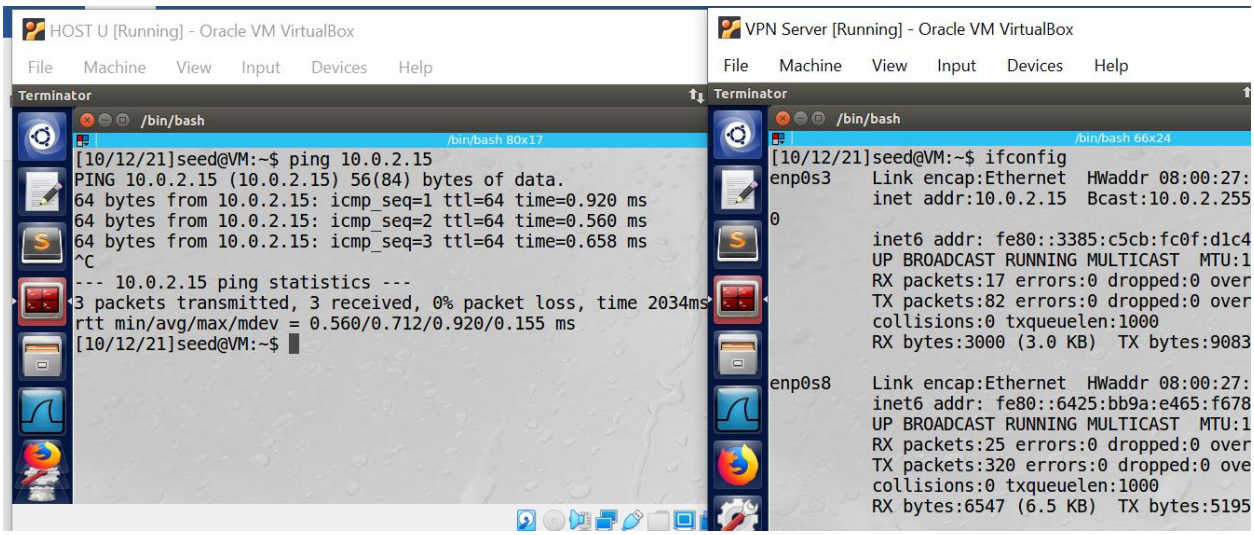

HOST V - Settings
General
System
Display
Storage
Audio
Network
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
intnet
Advanced


HOST U [Running] - Oracle VM VirtualBox
HOST V [Running] - Oracle VM VirtualBox
VPN Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu Desktop
Search your computer
HOST U
Running
SEEDLABS
Right Ctrl

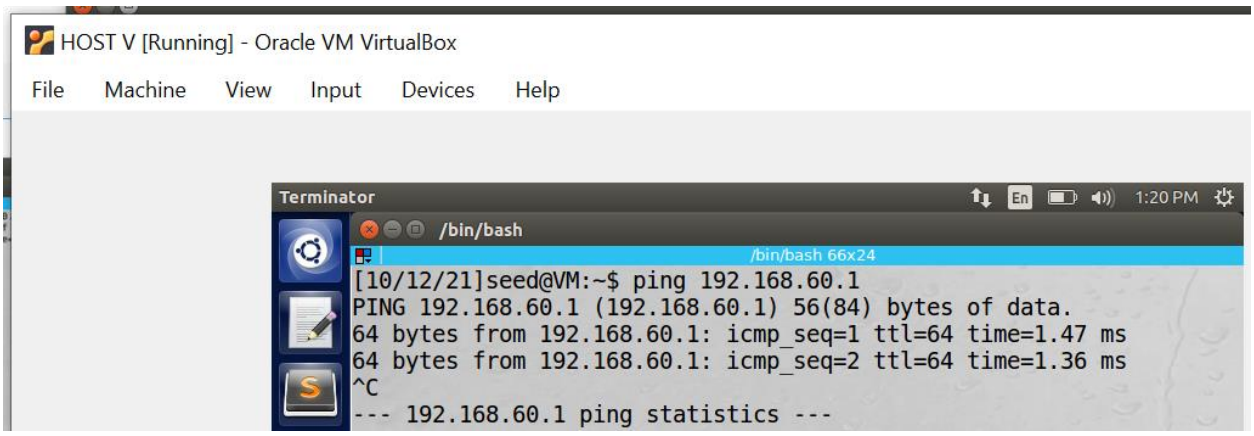
Host U can't ping host V, and they are not on the same network



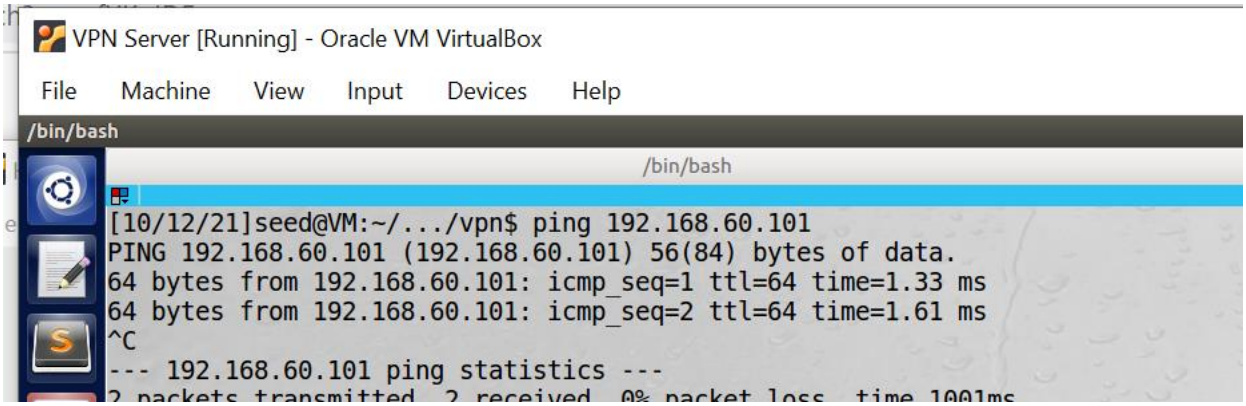
Host U can ping the server



And host V can ping the server



The VPN server can ping the two machines



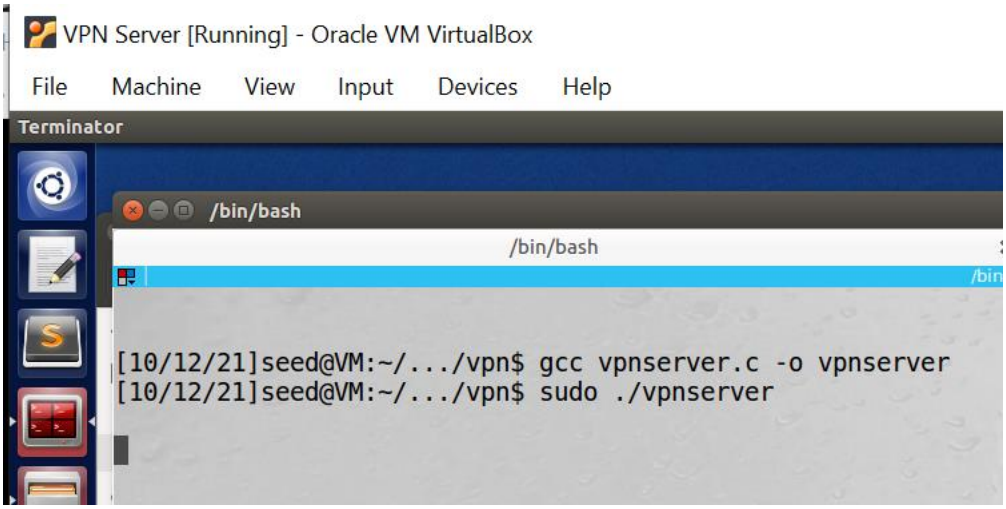
Task2

Creating a VPN Tunnel using TUN/TAP

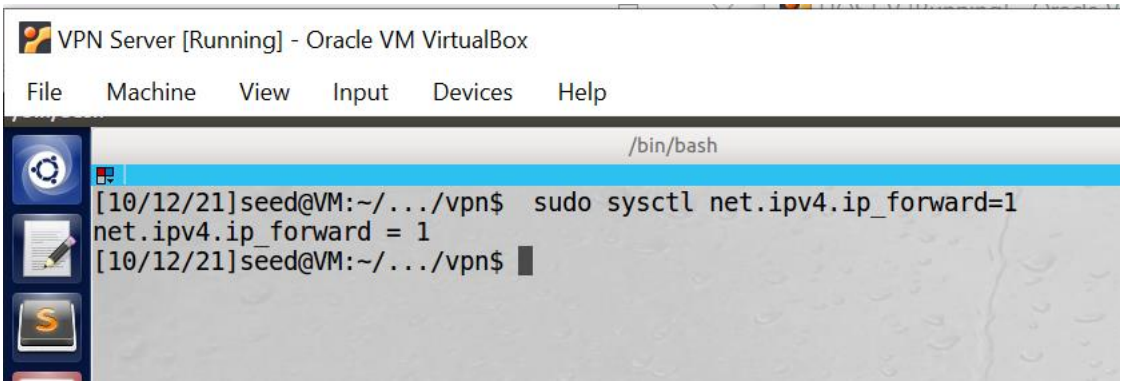
First, download the e VPN client program (vpnclient) and a server program (vpnserver) and unzipped them. The vpnclient and vpnserver programs are the two ends of a VPN tunnel. They communicate with each other using either TCP or UDP via the sockets depicted

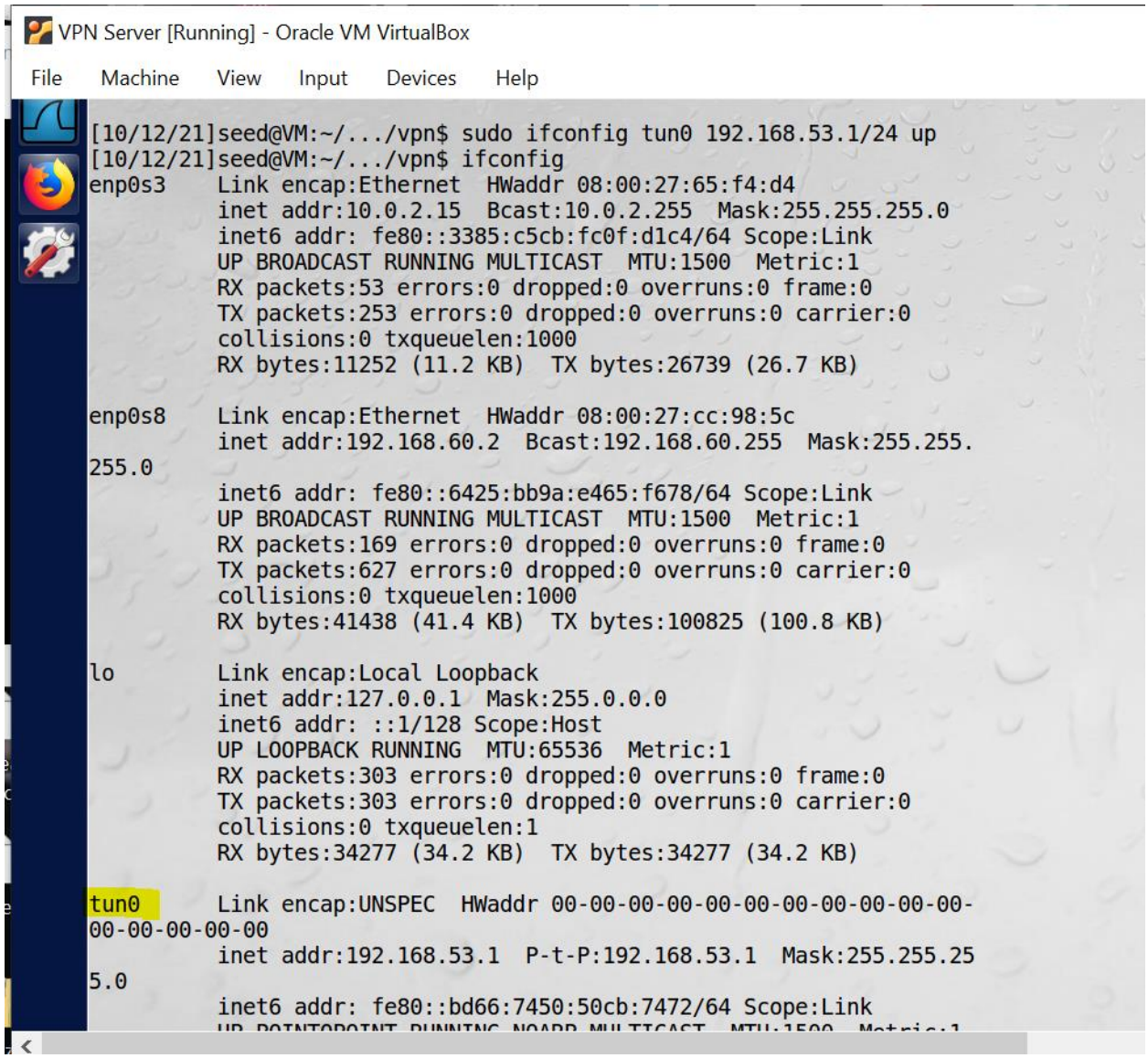
We run VPN Server. We first run the VPN server program vpnserver on the Server VM. After the program runs, a virtual TUN network interface will appear in the system.

Compile and run the vpnserver in the server machine

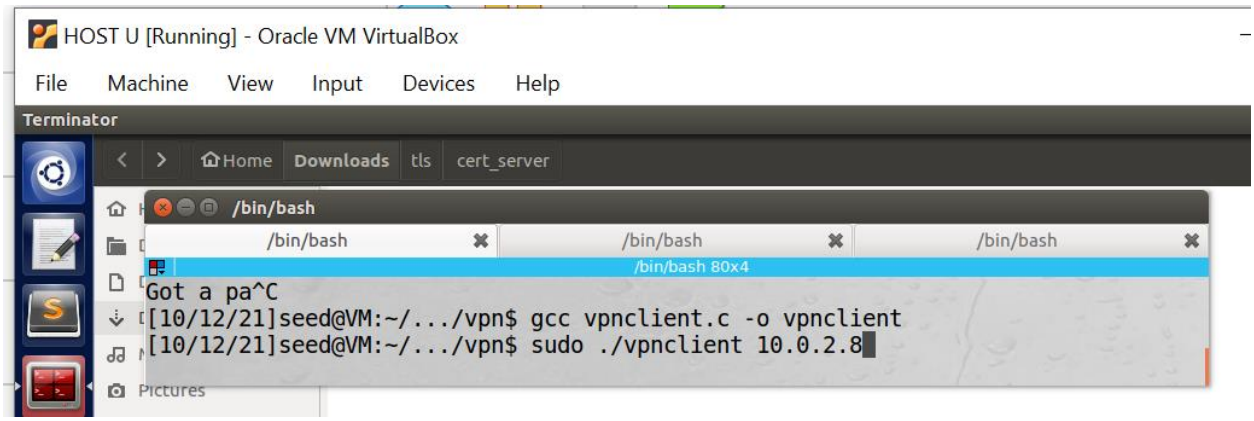


The VPN Server needs to forward packets between the private network and the tunnel, so it requires to function as a gateway.

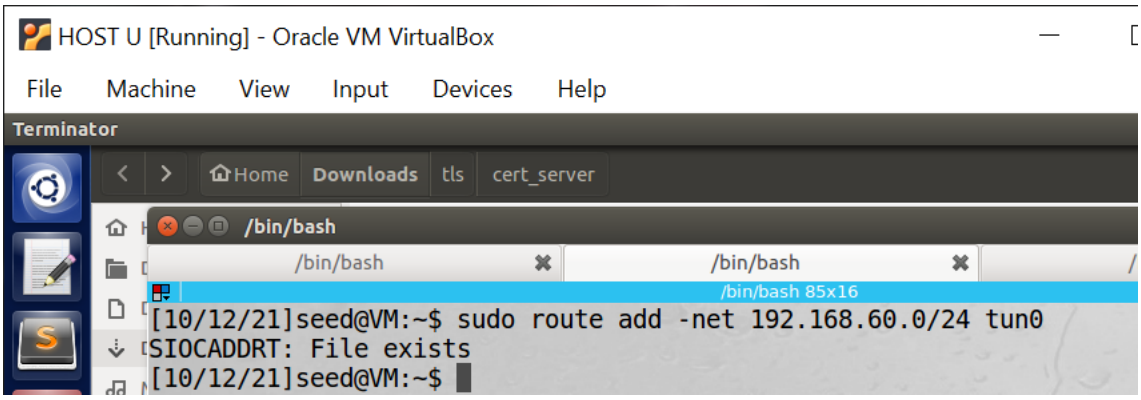


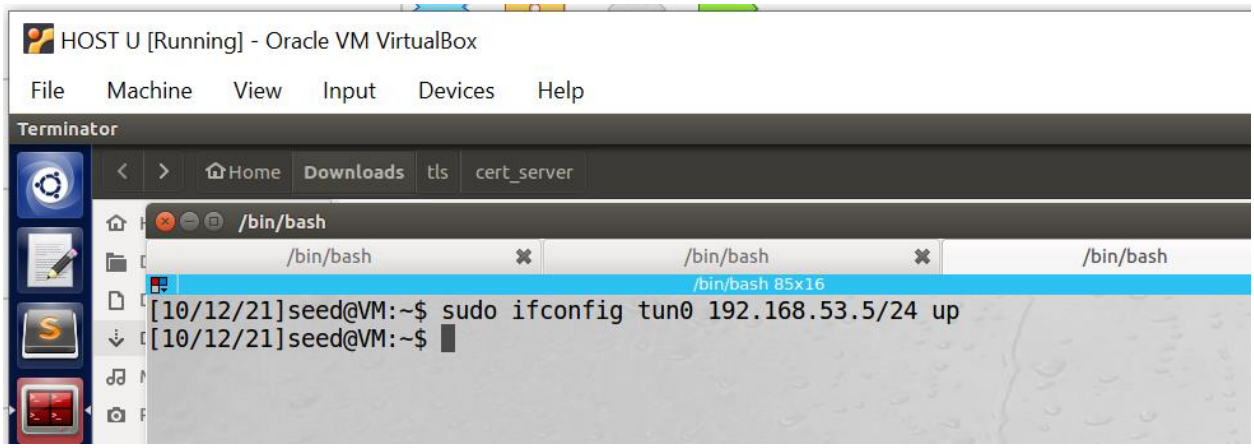


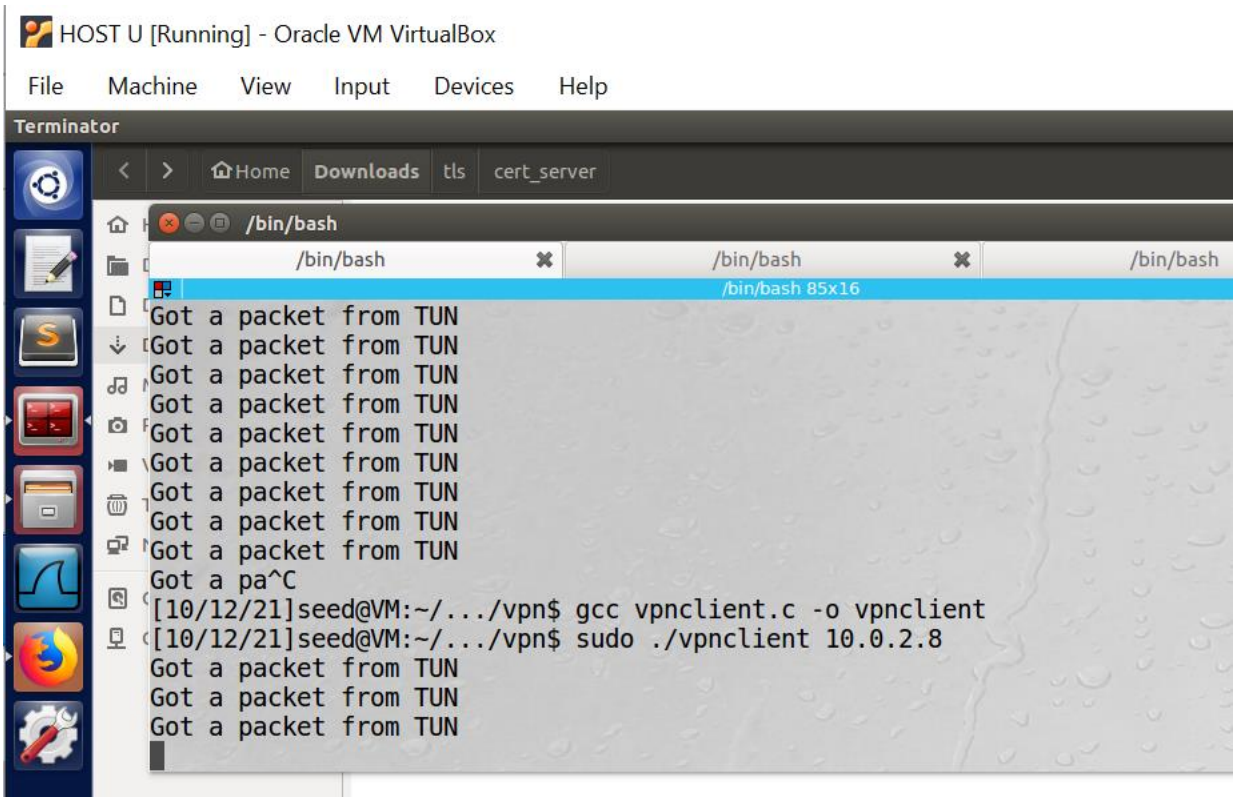
Then Run VPN Client. We now run the VPN client program on the Client VM machine U using the downloaded program



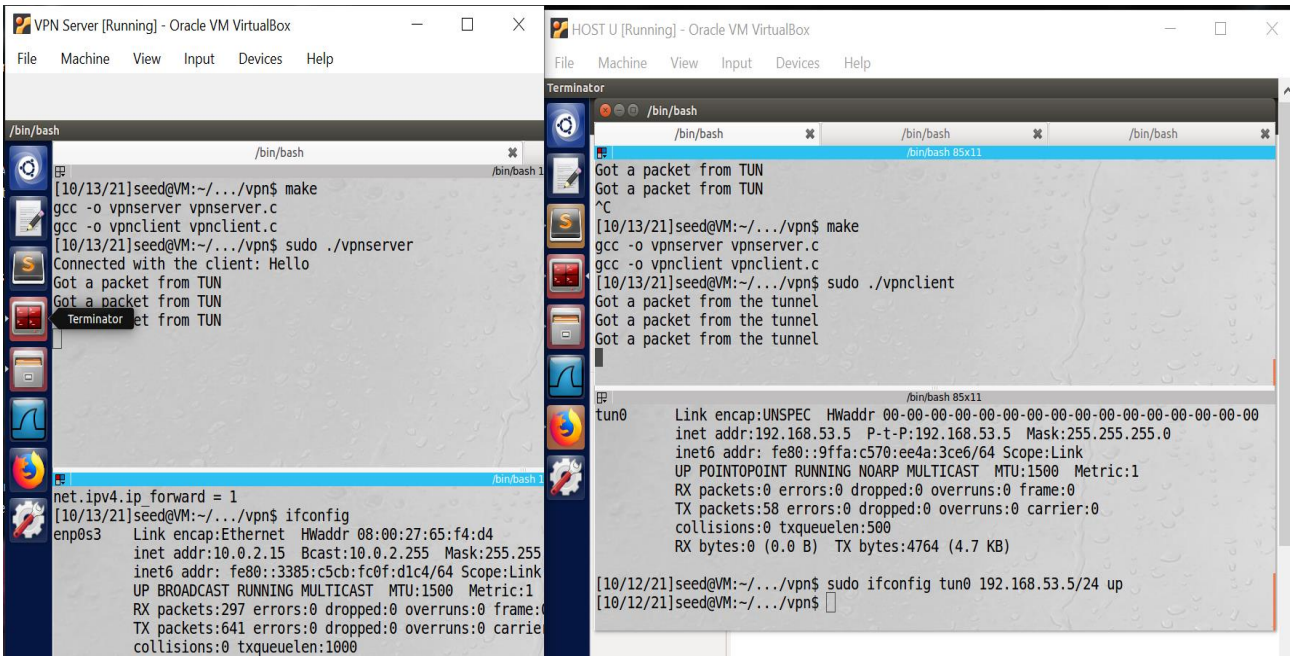
Set Up Routing on Client and Server VMs



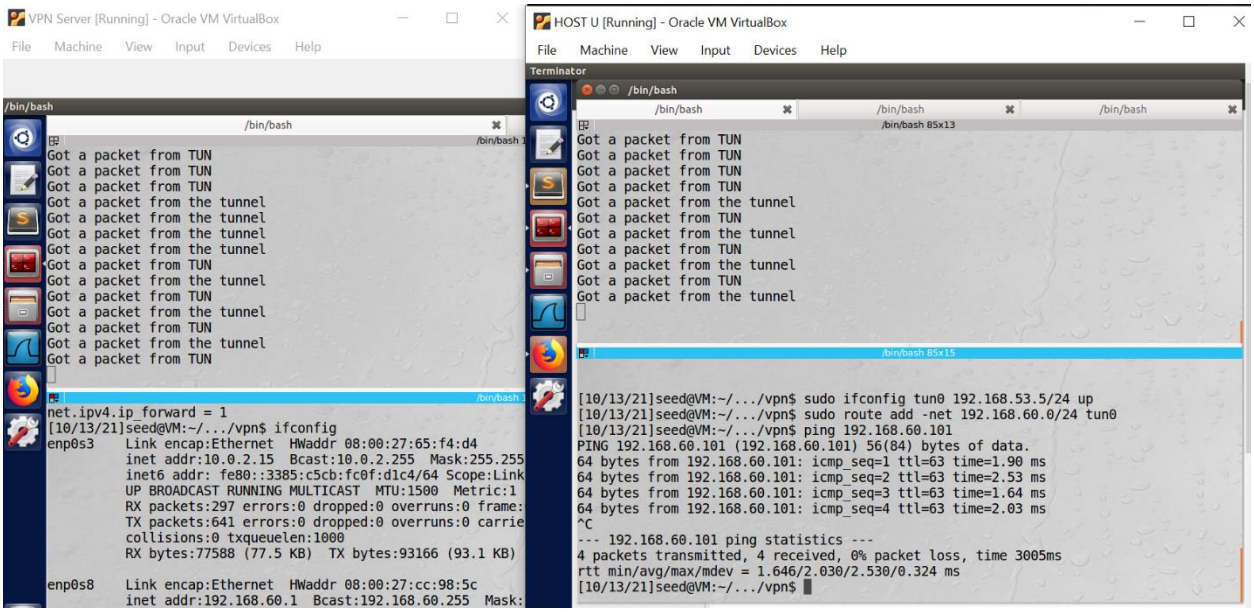




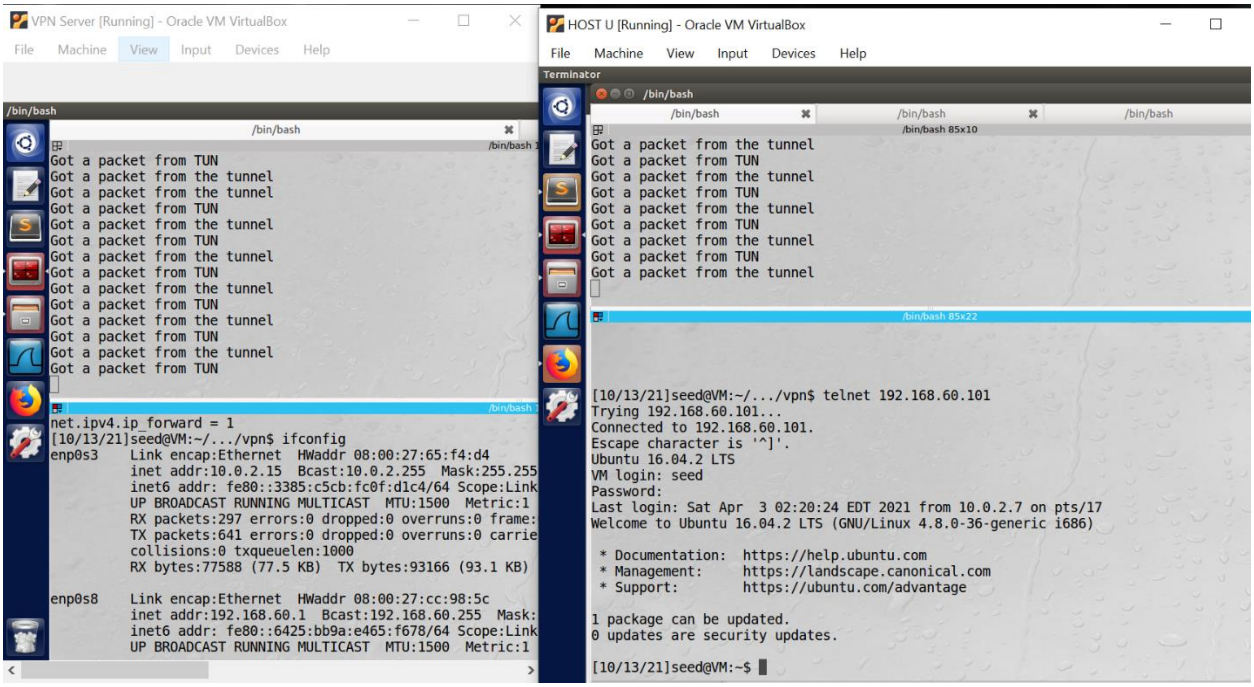
Here are the two machines the sever and machine U



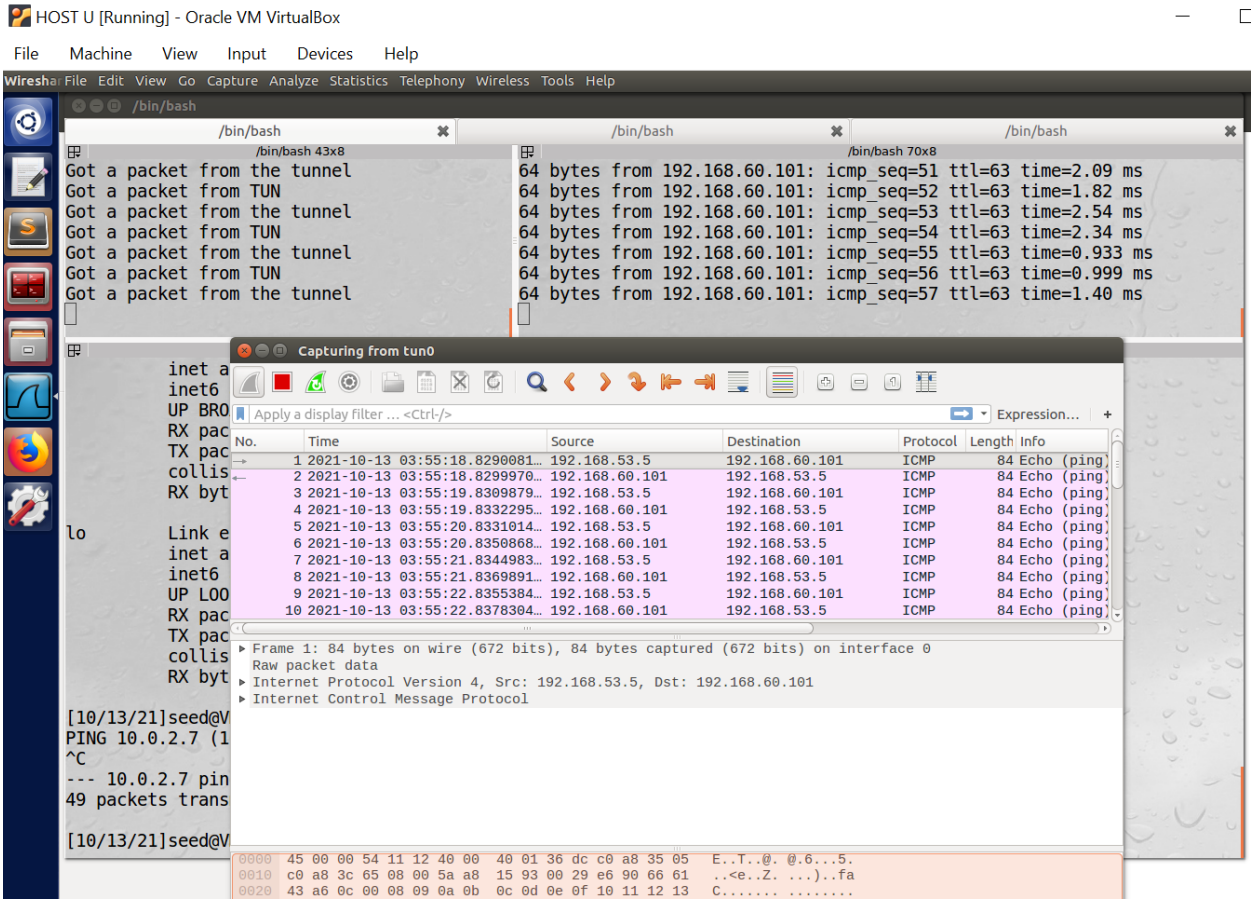
Test the VPN Tunnel by tying to ping the machine V from the machine U while they are not on the same network



And telnet the machine V from machine U

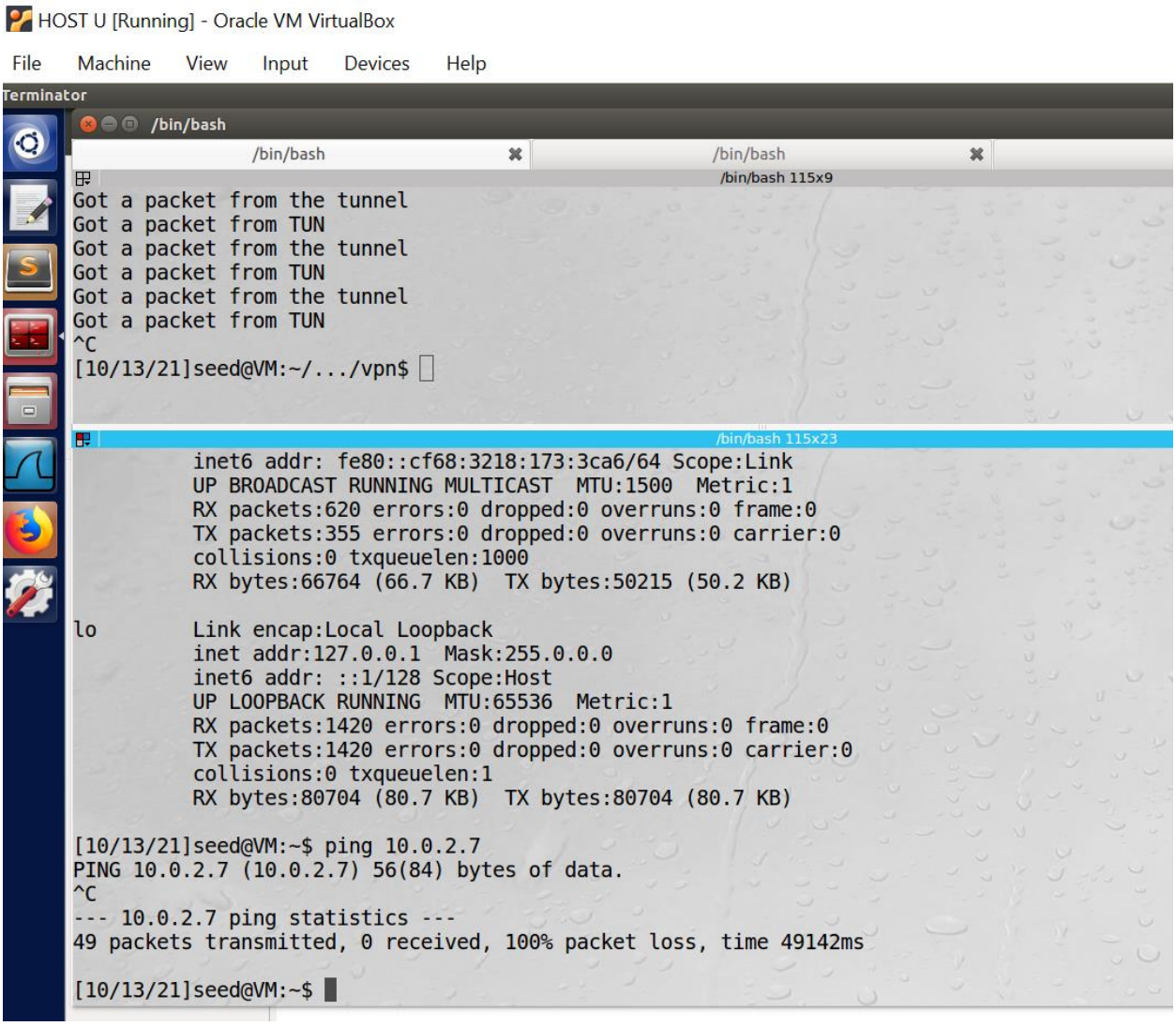


Wireshark to capture the network traffics on all the interfaces on the client VM



Tunnel-Breaking Test.

After breaking the tunnel, we can’t access machine V from machine U

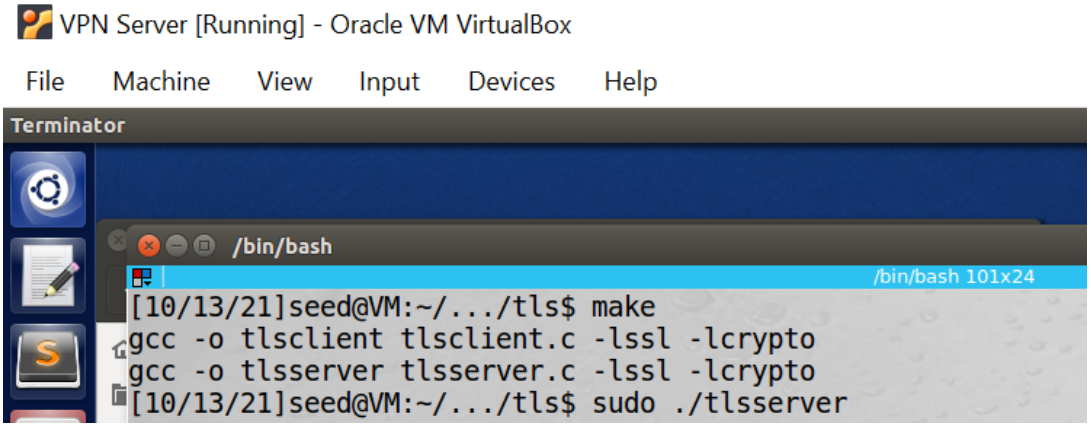

HOST U [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash
/bin/bash
/bin/bash 115x9
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
^C
[10/13/21]seed@VM:~/.../vpn$
/bin/bash 115x23
inet6 addr: fe80::cf68:3218:173:3ca6/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:620 errors:0 dropped:0 overruns:0 frame:0
TX packets:355 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:66764 (66.7 KB) TX bytes:50215 (50.2 KB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:1420 errors:0 dropped:0 overruns:0 frame:0
TX packets:1420 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:80704 (80.7 KB) TX bytes:80704 (80.7 KB)
[10/13/21]seed@VM:~$ ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
^C
--- 10.0.2.7 ping statistics ---
49 packets transmitted, 0 received, 100% packet loss, time 49142ms
[10/13/21]seed@VM:~$

Task 3 and 4: Encrypting the Tunnel, Authenticating the VPN Server

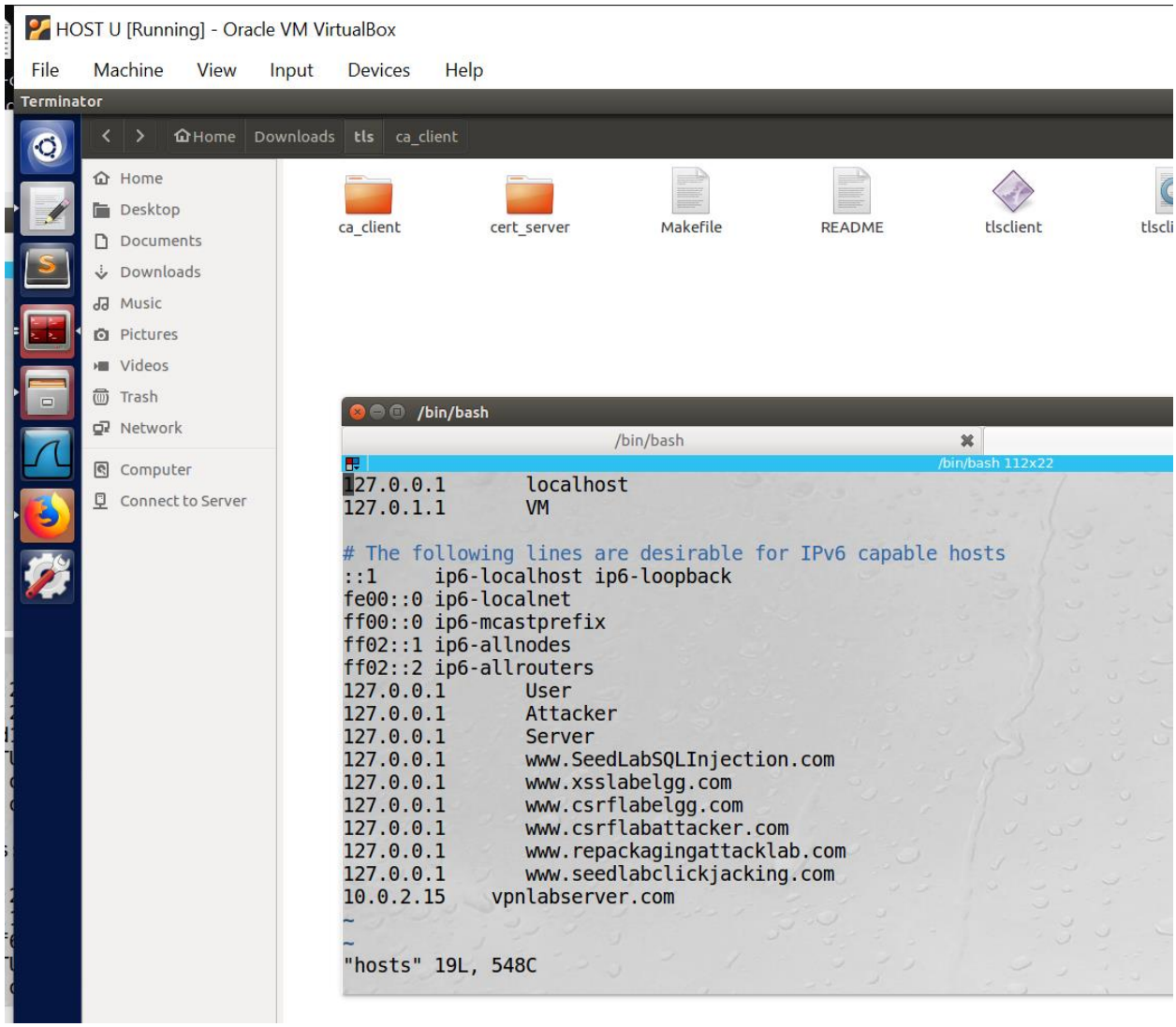
To secure this tunnel, we need to achieve two goals, confidentiality and integrity. The confidentiality is achieved using encryption, i.e., the contents that go through the tunnel is encrypted. The integrity goal ensures that nobody can tamper with the traffic in the tunnel or launch a replay attack. Integrity can be achieved using Message Authentication Code (MAC)

A sample TLS client and server program (tlsclient and tlsserver) is provided in a zip file that can be downloaded from the website

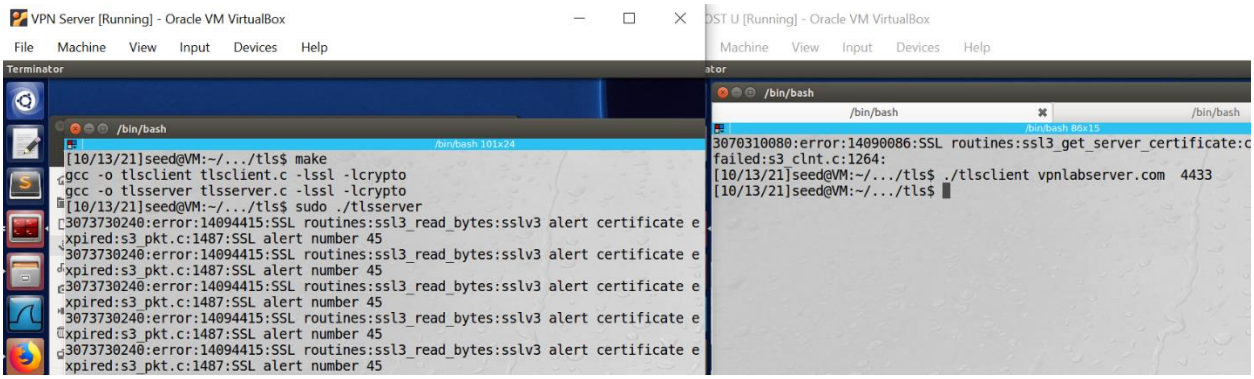
On the Server machine we compile and run the tlsserver program



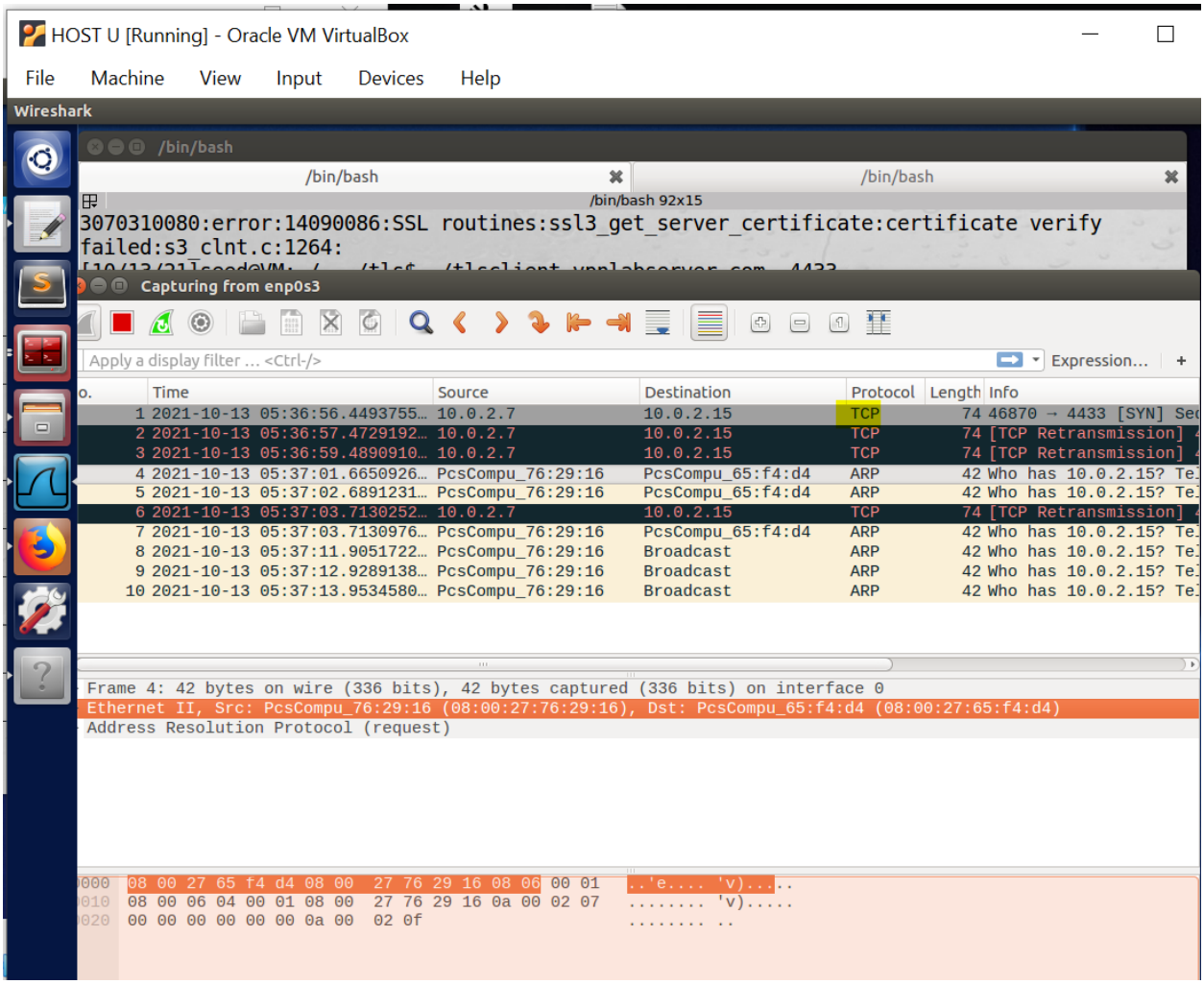
On the host U machine, we should first read the “ read me “ file to add the server IP and hostname to /etc/hosts as mentions in the file



Then after that we use the command that mentioned in the file and run the tlsclient program

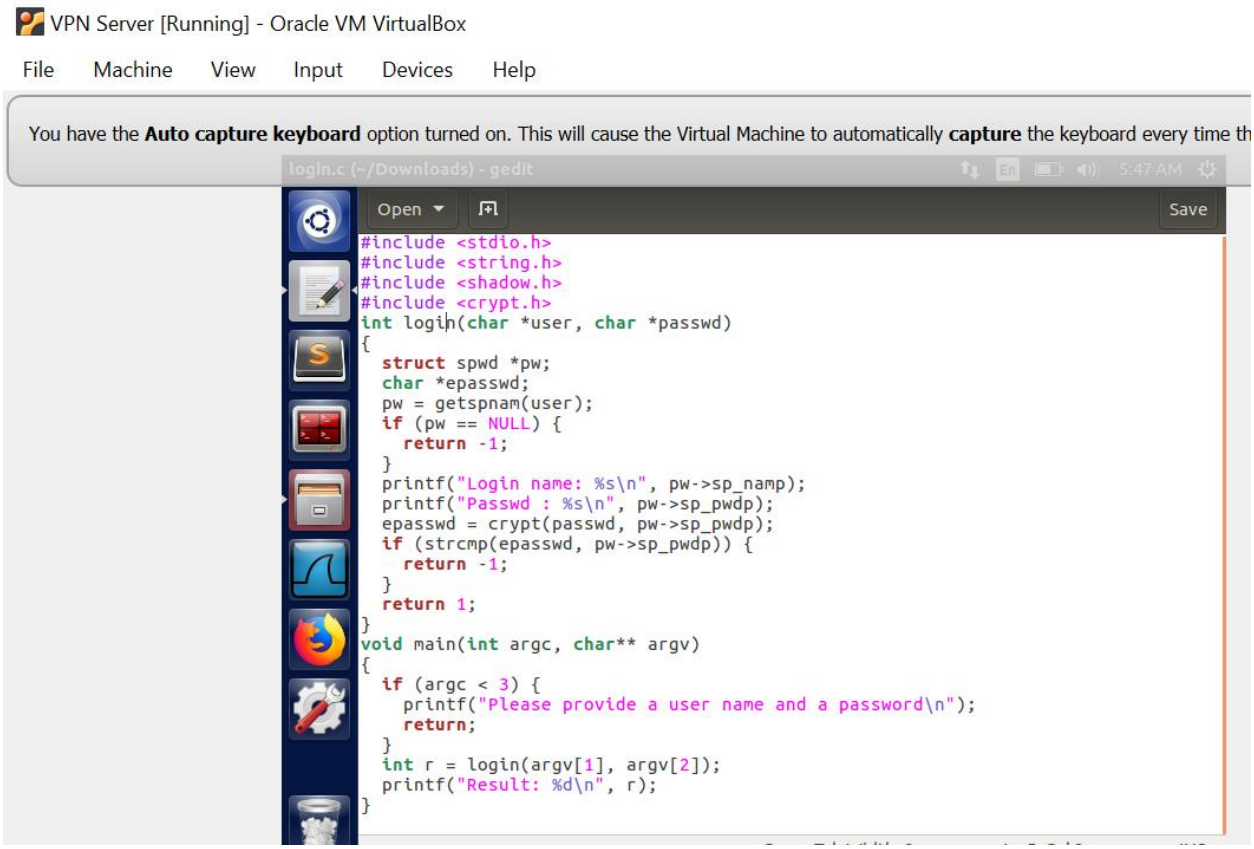


Start the wirshark to capture the network



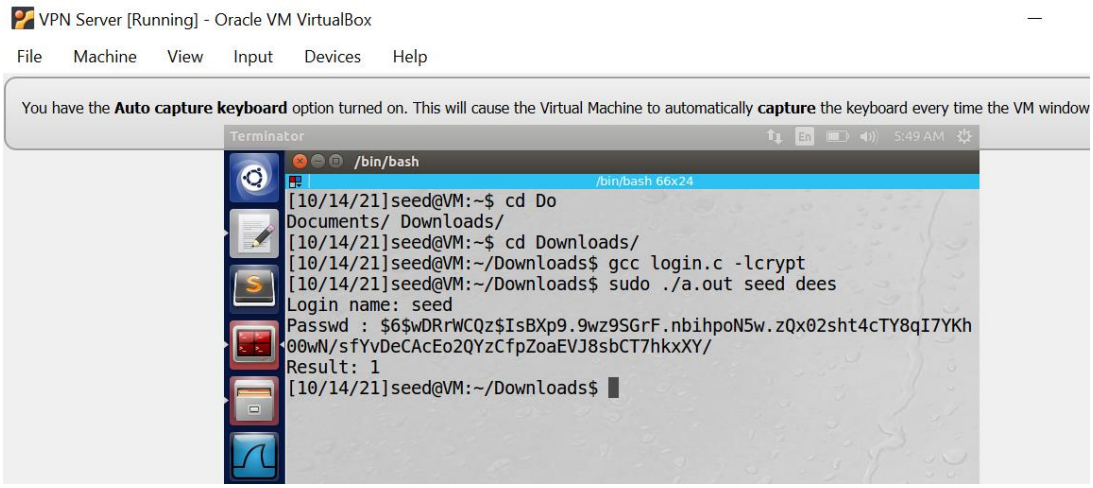
Task 5: Authenticating the VPN Client

Here are the code



We can compile the code above and run it with a user name and a password.

We use the seed and dees as password and username



Task 6: Supporting Multiple Clients

Linux has a system call called select(), which allows a program to monitor multiple file descriptors simultaneously

```
fd_set readFDSet;
int ret, sockfd, tunfd;

FD_ZERO(&readFDSet);
FD_SET(sockfd, &readFDSet);                                  ①
FD_SET(tunfd, &readFDSet);                                   ②
ret = select(FD_SETSIZE, &readFDSet, NULL, NULL, NULL);      ③

if (FD_ISSET(sockfd, &readFDSet){
        // Read data from sockfd, and do something.
}

if (FD_ISSET(tunfd, &readFDSet){
        // Read data from tunfd, and do something.
}
```